



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/084,436	02/28/2002	Zhichen Xu	10018744-1	6233
<div>7590 01/04/2007 HEWLETT-PACKARD COMPANY Intellectual Property Administration P.O. Box 272400 Fort Collins, CO 80527-2400</div>			<div>EXAMINER LEMMMA, SAMSON B</div>	
			<div>ART UNIT 2132</div>	<div>PAPER NUMBER</div>
SHORTENED STATUTORY PERIOD OF RESPONSE			MAIL DATE	DELIVERY MODE
2 MONTHS			01/04/2007	PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents  
United States Patent and Trademark Office  
P.O. Box 1450  
Alexandria, VA 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

**MAILED**

**JAN 04 2006**

**Technology Center 2100**

**BEFORE THE BOARD OF PATENT APPEALS  
AND INTERFERENCES**

Application Number: 10/084,436  
Filing Date: February 28, 2002  
Appellant(s): XU ET AL.

Timothy King Reg. No. 46,423  
For Appellant

**EXAMINER'S ANSWER**

This is in response to the appeal brief filed on 08/28/2006 appealing from the Office action mailed on 04/10/2006, finally rejecting claims 1-36.

Art Unit: 2132

**(1) Real Party in Interest**

A statement identifying by name the real party in interest is contained in the brief.

**2) Related Appeals and Interferences**

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

**(3) Status of Claims**

The statement of the status of claims contained in the brief is correct.

**(4) Status of Amendments After Final**

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

**(5) Summary of Claimed Subject Matter**

The summary of claimed subject matter contained in the brief is correct.

**(6) Grounds of Rejection to be Reviewed on Appeal**

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

**(7) Claims Appendix**

The copy of the appealed claims contained in the Appendix to the brief is correct.

**(8) Evidence Relied Upon**

Art Unit: 2132

5,862,223	Walker et al	01-1999
6,460,036	Herz	10-2002

### **(9) Grounds of Rejection**

The following ground(s) of rejection are applicable to the appealed claims:

### ***Claim Rejections - 35 USC § 103***

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:
2. **Claims 1-36** are rejected under 35 U.S.C. 103(a) as being unpatentable over Walker et al. (hereinafter referred as Walker) (U.S. Patent No 5,862,223) in view of Herz (hereinafter referred as Herz) ((U.S. Patent No 6,460,036) (filed on Dec 5, 1997)
3. **As per claim 1, 8,12,15,17-18, 24, 31-32 Walker discloses** a method of increasing peer privacy in a computer network including peers operable to exchange information via network, wherein the peers include computing platforms, [column 35, lines 14-17] the method comprising:
  - **Receiving a request for data from a data requester,**[column 35, 45-47; column 35, lines 15-17] (Bob's computer receives Alice request through the 3<sup>rd</sup> trusted party central controller/carol's computer as described on column 35, lines 33-34)

- **Determining whether a data provider exists that stores the requested data wherein the data provider is a peer of the peers;**[Abstract, figure 2, ref. Num "270";column 8, 22-27 and column 35, lines 29-67] (As explained on abstract, the present invention includes a controller having a database for storing expert qualifications. In one embodiment, the controller receives an expert request/requested data. A search program identifies experts qualified to respond to the expert request/requested data. The expert request/requested data is then transmitted **to the expert/data provider**, which results in **an expert answer transmitted** to and received by the central controller. As explained on column 8, lines 22-27, once the Exchange contains enough experts in a given subject, each new application may be reviewed by other experts who are already members of the Exchange. **This provides a basis for peer review** that can be used to maintain assurance of qualifications. As explained on column 35, line 32b, Bob's computer is also qualified expert. Bob's computer is acts as both client and server when interacts with carol's computer and is assumed to be a modern PC which meets the limitation of a peer and since there are a number of experts, the qualified expert who would be selected to provide the an expert answer, or Bob's computer meets the limitation of peer of peers and carol's computer or the central controller determines whether a data provider for instance Bob's computer exists that stores the requested data)

- **Selecting a plurality of peers to form a path between said data provider and said data requestor,**[Abstract, column 35, lines 14-17;column 36, lines 40-42; column 8, lines 52-53, experts/data providers/peers can be chosen or selected as disclosed on column 8, lines 52-53; therefore if the experts answers comes from a plurality of experts for the same data request, the controller will inherently form a path between said provider and data requestor] **wherein said data provider and said data**

Art Unit: 2132

**requester are the respective ends of said path;**[column 36, lines 40-42, column 35, lines 45-column 36, lines 42]

- **generating a mix according to said path, wherein the mix includes an anonymous identity of each of the plurality of peers in the path;**[Column 35, lines 14-18 and column 35, lines 19-30; column 36, lines 40-41] **and transmitting said mix to said data provider** [column 36, lines 9-10 and figure 29]. (carol's computer sends M\_1 to Bob/data provider via anonymous mix 180 meets the limitation of transmitting said mix to said data provider.)

**Walker** does not explicitly disclose generating a mix according to said path

However, in the field of endeavor Herz discloses

- **Generating a mix according to said path wherein the mix includes an anonymous identity of each of the plurality of peers in the path.**[column 39, lines 3-17; lines 18-23 and column 39, line 66-column 40, line 6; column 37, lines 50-52; column 39, lines 3-7]

**Furthermore, Herz discloses determining whether a data provider exists that stores the requested data wherein the data provider is a peer of the peers;**[column 38, lines 39-42; figure 2, ref. Num "S4"; column 38, lines 31-47]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of generating a mix according to the path wherein the mix includes an anonymous identity of each of the plurality of peers in the path as per teachings of Herz in to the method as taught by **Walker**, in order to provide a secure communication and protection against eavesdropper.[See Herz, column 39, lines 8-line 17 and column 40, lines 3-6]

Art Unit: 2132

4. **As per claims 2,16,19 and 25 the combination of Walker and Herz discloses** a method as applied to claim above. Furthermore Walker discloses the method further comprising: generating a first encryption key; and encrypting said first encryption key with a public encryption key of said data provider. **[[column 35, lines 63-column 36, line 6]]**(The first encryption key is a key k<sub>3</sub> is generated by carol/the 3<sup>rd</sup> trusted peer/computer and the first encryption key generated by carol which is K<sub>3</sub> is also protected or encrypted with the public key of Bob as shown on column 36, lines 3, x<sub>3</sub>, and line 11)

5. **As per claims 9-11,13-14, 33-36 Walker discloses a method of increasing peer privacy in a computer network including peers operable to exchange information via the network, wherein the peers include computing platforms,** [column 36, lines 40-41; column 35, lines 14-28 and column 35, line 29-column 36, line 41] **the method comprising:**

**receiving a message comprising a mix at a current peer, wherein the mix includes an anonymous identity of each of a plurality of peers in a path between a data provider and a data requestor in the network**[column 36, lines 40-41, column 35, lines 63, carol receives message comprising mix from Alice]; **modifying said mix by applying a complementary encryption key of said current peer to said mix;**[column 36, lines 7, M<sub>1</sub> which modifies said mix by applying encryption key] **retrieving a subsequent peer to said current peer; modifying said message with said modified mix; and transmitting said modified message to said subsequent peer.**[column 36, lines 11, c, carlos after retrieving a subsequent peer/bob to said current peer/carol; it modifies said message with said modified mix and send it to subsequent peer bob as it is described on column 35, lines 63-column 36, lines 11 and figure 29]

**Walker** does not explicitly disclose generating a mix according to said path

However, in the field of endeavor Herz discloses

Art Unit: 2132

**Generating a mix according to said path wherein the mix includes an anonymous identity of each of the plurality of peers in the path.**[column 39, lines 3-17; lines 18-23 and column 39, line 66-column 40, line 6; column 37, lines 50-52; column 39, lines 3-7]

**Furthermore, Herz discloses determining whether a data provider exists that stores the requested data wherein the data provider is a peer of the peers;**[column 38, lines 39-42; figure 2, ref. Num "S4"; column 38, lines 31-47]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of generating a mix according to the path wherein the mix includes an anonymous identity of each of the plurality of peers in the path as per teachings of Herz in to the method as taught by **Walker**, in order to provide a secure communication and protection against eavesdropper.[See Herz, column 39, lines 8-line 17 and column 40, lines 3-6]

6. **As per claims 3-7, 20-23 and 26- 30 Walker discloses** an apparatus for increasing privacy in a computer network including peers operable to exchange information via the network, wherein the peers include computing platforms, the apparatus comprising:

at least one processor; [figure 2, ref. Num "205" and figure 4, "405"]

memory coupled to said at least one processor; [figure 2, 215 & 220]

and a privacy module residing in said memory and said privacy module executed by said at least one processor, wherein said privacy module is configured to receive a message at said data provider [figure 2, 210], said message comprises:

A mix configured to provide a path among a plurality of the peers between a data provider and a data requestor in the network, wherein the mix includes an



Art Unit: 2132

anonymous identity of each of the plurality of peers in the path [Column 35, lines 14-18; column 36, lines 40-41; Column 35, lines 14-18 and column 35, lines 19-30; column 36, lines 40-41] ;

**an encrypted reference to requested data encrypted with a first encryption key [column 35, lines 63-column 36, line 6]**(the first encryption key is a key generated by carol K\_3/the 3<sup>rd</sup> trusted peer/computer and the reference N shown on column 36, lines 1, which is included in the message from Alice is encrypted as shown on column 36, lines 6 (X\_4)); **an encrypted first encryption key protected with a public key of said data requester;** [Column 35, lines 36-column 36, line 10] (encrypted first encryption key generated by carol which is K\_3 is also protected or encrypted with the public key of Bob) **and said privacy module is also configured to decrypt said first encryption key with a complementary encryption key to said public key of said data provider [column 36, lines 11-13]** (Bob receives M\_1 and decrypt the first encryption key K\_3 with a complementary/private key of BOB) and decrypts said data reference with said encryption key and once he gets the decrypted first encryption key K\_3, he decrypts the X\_4, included in the message to verify the signature. Therefore the N which meets the limitation of end user request identifier is decrypted.)

**Walker** does not explicitly disclose a mix configured to provide a path

However, in the field of endeavor Herz discloses

**A mix configured to provide a path wherein the mix includes an anonymous identity of each of the plurality of peers in the path.**[column 39, lines 3-17; lines 18-23 and column 39, line 66-column 40, line 6; column 37, lines 50-52; column 39, lines 3-7]

Art Unit: 2132

**Furthermore Herz discloses,**

The user's client processor C3 forms a signed message **S(R, SK.sub.P)**, which is paired with the user's pseudonym P and (if the request R requires a response) a secure one-time set of return envelopes, to form a message M. It protects the message M with a multiply enveloped route for the outgoing path. The enveloped route s provide for secure communication **between S1 and the proxy server S2**. The message M is enveloped in the most deeply nested message and is therefore difficult to recover should the message be intercepted by an eavesdropper. 2. The message M is sent by client C3 to its local server S1, and is then routed by the data communication network. **N from server S1 through a set of mixes as dictated by the outgoing envelope set and arrives at the selected proxy server S2**. 3. The proxy server **S2 separates the received message M into the request message R, the pseudonym P, and (if included) the set of envelopes for the return path. The proxy server S2 uses pseudonym P to index and retrieve the corresponding record in proxy server S2's database**, which record is stored in local storage at the proxy server S2 or on other distributed storage media accessible to. proxy server S2 via the network N. This, record contains a public key PK.sub.P, user-specific information, and credentials associated with pseudonym P. The proxy server S2 uses the public key PK.sub.P to check that the signed version S(R, SK.sub.P) of request message R is valid. [column 39, lines 8-35]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of **configuring a mix to provide a path** wherein the mix includes an anonymous identity of each of the plurality of peers in the path as per teachings of Herz in to the method as taught by **Walker**, in order to provide a secure communication and protection against eavesdropper.[See Herz, column 39, lines 8-line 17 and column 40, lines 3-6]

Art Unit: 2132

**(10) Response to Argument**

Appellant's argument filed with the Appeal brief, on April 24, 2006 have been fully considered but they are not persuasive.

**Referring to the independent claim 1, Rejections - 35 USC § 103 (a), Appellant argued** that the following limitation recited in respective independent claim 1, **"determining whether a data provider exists that stores the requested data"**, is neither disclosed by the primary reference Walker nor by the secondary reference Herz.

**Appellant wrote the following in support of his argument.**

*"A controller, such as a person (ie., Carol), in Walker receives an expert request/requested data and a search program identifies an expert, such as Bob, qualified to respond to the experts. Walker discloses selecting an expert qualified to respond to a request. However, Walker fails to teach or suggest determining whether a computer stores the requested data. Selecting a qualified expert is not the same as determining whether a computer exists that stores the requested data. Claim 1 does not recite selecting a qualified expert or selecting a qualified expert's computer. Instead, claim 1 recites determining whether a data provider (i.e., computing platform) exists that stores the requested data. Walker only discloses selecting an expert that is allegedly qualified to respond to a request, but does not determine whether the expert stores requested data in a computer or otherwise knows the answer to a request. Simply because an expert in Walker may store an answer in his/her computer after determining the answer does not require making a determination of whether an expert's computer exists which stores the answer."*

**Examiner disagrees with this argument.**

In response to the appellant's argument that the primary reference namely Walker fail to show **determining whether a data provider (i.e., computing platform) exists that stores the requested data**, examiner would like to point out that walker on column 18, lines 23-30 discloses the following.

“ In another embodiment, expertise is provided not by a human expert, but by

**conventional expert system, neural network, or software using artificial intelligence.** An expert system specializing in the diagnosis of blood disorders, for example, could perform key word searches on end user requests 120. These key words would become the input parameters upon which the expert system would base its decision.”

Furthermore, examiner would point out that, before the central controller routes user request for appropriate/qualified experts, which could be expert system as shown above [see column 19, lines 1-3 and figure 7, ref. Num 710], the controller, searches a similar request in database. This is disclosed by Walker as follows.

**“Before searching for the appropriate expert to respond to end user request 120,** central controller 200 **searches end user request database 265 at step 710 for similar end user requests 120** so that unnecessary duplication of work by experts is not performed. If end user request 120 relates to tax strategies for small businesses and has been asked before, there may be no need for having an expert create a new expert answer 130. It is simpler and cheaper to use the existing expert answer 130.

Conventional search algorithms are used to search end user request database 265 for **duplicate or similar end user requests 120.** Examples of such string search algorithms include Knuth-Morris-Pratt, Rabin-Karp, Boyer-Moore, and Baeza-Yates-Gonnet. For reference, one of ordinary skill in the art may refer to Thomas H. Cormen, et al, Introduction to Algorithms, (MIT Press, 1990). Such algorithms could be used to **determine a match so that end user requests 120 using different formats and sentence structure can be found.** If a similar end user request 120 is found at step 720, then the end user is given the option of purchasing the associated expert answer 130 at step 730. If the end user wants to buy it, expert answer 130 is transmitted to the end user at step 740. A bill is sent to the end user at step 750, and royalty payments

are added to the account of the **expert who generated expert answer 130**" [column 19, lines 66-column 20, line 22].

This implies the fact that based on the user request, the controller **would determine whether a data provider (i.e., computing platform) or expert system exists that stores or generates the requested data/expert answer**. If it happens to be the expert system that is in the first place generates the requested data, then it has to be some sort of computer loaded **with in-depth knowledge of specific subject**. This is simply because expert system is nothing but a knowledge-based applications of artificial intelligence, which performs tasks, based on the knowledge stored in its database. Human performs using their intelligence and Expert system performs similar tasks based on **particular knowledge stored in their system**.

Examiner would further indicate that on column 20, lines 28-49 and column 20, lines 66- column 20, line 1 and on column 21, lines 9-11, Walker further discloses the following, which is relevant for the above appellant's argument.

"Referring again to FIG. 7, if a similar end user request 120 is not found at step 720, or if the end user decides not to buy expert answer 130 at step 730, **then central controller 200 begins to search for appropriate candidate experts satisfying criteria 117**. At step 760, criteria 117 of end user request 120 are extracted and used as parameters **for a search of expert database 255**. At step 770, **a list of experts** is generated whose qualifications meet criteria 117. In a simple example, criteria 117 is "SUBJECT=mathematics and LEVEL=4 and PAPERS=number theory." Central controller 200 searches expert qualifications database 285 for all records with expert qualifications 140 field value of level four mathematician. From this subset of experts, the database field for publications is then searched, **eliminating all experts who have not published in number theory. The resulting list of experts satisfies criteria 117**. Those skilled in the art will appreciate that there are many database search techniques

Art Unit: 2132

in addition to those protocols described above. Fuzzy logic protocols, expert systems, and other systems using artificial intelligence may also be used to search the database and **identify experts who have expert qualifications 140 which correspond to criteria 117.**" [Column 20, lines 28-49]

"The resulting list of candidate experts may also be reduced after examining expert profiles **155 stored in expert database 255.**" [Column 20, lines 66-column 21, line 1]

"These requirements are codified into rules and relationships which can be executed by central controller 200, narrowing the list of target experts" [Column 21, lines 9-11]

**Therefore from what is disclosed above, it is clear that the controller selects only few experts/ expert systems, among a list of appropriate/qualified candidate experts, satisfying a particular criteria. This is equivalent to,** determining whether a data provider /expert/expert system (i.e., computing platform) exists that stores the requested data, and finally forwarding the request only to the selected expert systems. For one of ordinary skill in the art the reason why the controller goes through the above selection process, **is to determine which data provider /expert/expert system (i.e., computing platform), stores the appropriate answer/ requested data and forward the request only to those which are determined to have the requested data.** And this meets the limitation of determining whether a data provider /expert/expert system (i.e., computing platform) exists that stores the requested data.

**Referring to the independent claim 1, Appellant's next argument** is referring to the following limitation recited in respective independent claim 1, "selecting a plurality of the peers to form a path between said data provider and said data requestor, wherein

said data provider and said data requestor are the respective ends of the said path”.

**Appellant** argued that such limitation is neither disclosed by the primary reference Walker nor by the secondary reference Hertz.

**Appellant on page 12 of the appeal brief wrote the following, in support of his argument.**

*“Walker fails to teach or suggest selecting a plurality of peers between a data provider and a data requestor. Columns 35-36 of Walker describe an example of submitting and responding to an end user request. Alice the end user submits a request to the trusted third party/central controller, Carol. Carol selects an expert, Bob, for responding to the request. Carol sends the request to Bob, Bob sends the answer to Carol and Carol sends the answer to Alice. The path in Walker only includes a single person, Carol, between data provider, Bob, and the data requestor, Alice. Thus, Walker fails to teach or suggest selecting a plurality of peers between a data provider and a data requestor.”*

*“The rejection alleges that selecting a plurality of the peers is inherent in Walker Because if the expert answers come from a plurality of experts for the same data request, the controller will inherently form a path between said provider and data requestor. On the contrary, the controller may simply forward the answers from each experts to the requestor. However, the controller does not select a plurality of peers to be used between the data provider and the data requestor for transmitting the requested data to the data requestor. In claim 1, the plurality of peers to be used in a path between the data provider and the data requestor are pre-selected, and then included in a mix which is transmitted to the data provider. The controller in Walker does not pre-select a plurality of peers between the data provider and the data requestor for use in the path.”*

**Examiner disagrees with this argument.**

In response to the appellant’s argument that the primary reference namely Walker

Art Unit: 2132

fail to show the limitation, "selecting a plurality of the peers to form a path between said data provider and said data requestor, wherein said data provider and said data requestor are the respective ends of the said path", examiner would like to point out that walker on column 35, lines 1 – 29, discloses the following.

"Another embodiment of the present invention **uses anonymous mix 180 as part of a protocol to maintain anonymity between two people using a trusted third party, such as central controller 200 using public-key cryptography for encryption and digital signatures.** The exact algorithms are unimportant at the protocol level. All **public keys are signed by a certification authority like central controller 200.** Certificates can be sent with messages and different keys can be used for encryption and digital signatures. **The trusted third party knows everyone's public key and everyone knows the third party's public key. Anonymous mix 180 either knows everyone's public keys or their public keys are sent along with their identities.** Everyone is assumed to know anonymous mix 180's public keys. An example of the trusted third party protocol is illustrated below."

**As appellant admits on his page 14, last 3 lines of argument.** The data sent to the requestor may follow a network path when transmitted to the requestor. The routing protocol may determine the path as the data is being routed to the request. For one of ordinary skill in the art it is clear that if the requestor and the data providers are far to each other, there has to be some intermediate routers/peers that the path should follow before it finally reaches its destination. Thus, this meets the limitation, "selecting a plurality of the peers to form a path between said data provider and said data requestor, wherein said data provider and said data requestor are the respective ends of the said path"

Furthermore, Applicant did not argue the possibility that for the same request as long as the requester is willing to pay the bill, the expert answer could come from



Art Unit: 2132

two different experts for one and the same request. It is equivalent to a patient goes to two different doctors to get two different opinions, or even to three doctors to get triple opinions. In order to accommodate that possibility, the controller somehow should from a plurality of a path to route the requested data to the requestors and this also meets the limitation of "selecting a plurality of the peers to form a path between said data provider and said data requestor, wherein said data provider and said data requestor are the respective ends of the said path"

**Examiner would also point out** that what is described on column 35, lines 35-36, of the primary reference is just an example, and **does not in any way limit that the path in Walker to only include a single person**, Carol, between data provider, Bob, and the data requestor, Alice.

**Referring to the independent claim 1**, Appellant further argues that the following limitation recited in respective independent claim 1, "generating a mix according to said path, wherein the mix includes identity of the plurality of peers in the path; and transmitting said mix to said data provider", is neither disclosed by the primary reference Walker nor by the secondary reference Hertz.

**Appellant on page 15 of the appeal brief wrote the following, in support of his argument.**

*"Mixes are described in Herz as an anonymizing mix protocol as taught by D. Chaum in the paper titled "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", communications of the ACM, Volume 24, Number 2, February 1981. **This mix procedure provides untraceable secure anonymous mail between two parties with blind return addresses through a set of forwarding and return mounting servers termed "mixes". See column 34, line 61-column 35, line 40.**"*

*"Hertz however, fails to teach or suggest that the mix protocol includes selecting all the serves or peers in the path before transmitting the mail through **a set of forwarding and return mounting servers termed "mixes"**. Instead, the mix protocol may anonymously select servers or peers in the path as the data is transmitted. Claim 1 recites selecting the peers form the path and generating the mix from the selected peers, and then transmitting the mix to the data provider. Thus, the peers for the path are pre selected and the mix is generated from the pre-selected peers and them the entire mix is transmitted to the data provider so the data provider can use the mix to send the requested data to the data requestor. The mix procedure of Hertz **does not disclose pre-selecting the peers to be used in the mix.**"*

**Examiner disagrees with this argument.**

In response to the appellant's above argument, the examiner would like to point out that the primary reference namely Walker, as is explained above in the examiner's argument discloses the selection of the peers to be used in the mix.

Furthermore, examiner would indicate the fact that Herz also discloses the following, which is relevant to the above argument.

"In our system, the organizations that the user U interacts with are the **servers S1-Sn on the network N**. However, rather than directly corresponding with each server, the user employs a proxy server, e.g. S2, as an intermediary between the local server of the user s own client and the information provider or network vendor. **Mix paths as described** by D.Chaum in the paper titled Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms...." [Column 37, lines 21-45]

"The user forms a request to establish pseudonym P on proxy server S2, by sending the signed pseudonym S(P, SK.sub.Z) to the proxy server S2 along with a request to create a new database entry, indexed by P, and the public key PK.sub.P. **It envelopes the**

**message and transmits it to a proxy server S2 through an anonymizing mix path, along with an anonymous return envelope header 2". [Column 37, lines 45-52]**

"Regardless of the content of request R, the user, at client C3, initiates a connection to the user's local server S1, and **instructs server S1 to send the request R along a secure mix path to the proxy server S2**, initiating the following sequence of actions:

1. The user's client processor C3 forms a signed message  $S(R, SK.sub.P)$ , which is paired with the user's pseudonym P and (if the request R requires a response) a secure one-time set of return envelopes, to form a message M. It protects the message M **with multiply enveloped route for the outgoing path. The enveloped routes provide for secure communication between S1 and the proxy server S2.** The message M is enveloped in the **most deeply nested message and is therefore difficult to recover should the message be intercepted by an eavesdropper.** 2. The message M is sent by client C3 to its local server S1, and is then routed by the data communication network. N from server S1 **through a set of mixes as dictated by the outgoing envelope set and arrives at the selected proxy server S2."** [Column 39, lines 3-23]

"The proxy server S2, upon receipt of the response M2, creates a return message Mr comprising the response M2 **embedded in the return envelope set that was earlier transmitted to proxy server S2 by the user in the original message M.** It transmits the return message Mr along the pseudonymous **mix path specified by this return envelope set**, so that the response M2 reaches the user at the user's client processor C3" [column 39, lines 66- column 40, lines 6].

Therefore as it indicated above the mix procedure of Herz discloses pre-selecting the peers to be used in the mix, because the message is transmitted/returned along the pseudonymous **mix path specified by this return envelope set.**

As to the appellant's argument regarding the motivation to make the proposed combination by the examiner, **the examiner** would indicate that the test for obviousness is not whether the features of the references may be bodily incorporated into the other to produce the claimed subject matter but simply what the references make obvious to one of ordinary skill in the art. See *In re Bozek*, 163 USPQ 545. (CCPA 1969); *In re Richman* 165 USPQ 509, (CCPA 1970); *In re Beckum* 169 USPQ 47 (CCPA 1971).

The rest of arguments presented by the Appellant, referring to the rest of the independent claims are the same as that are already described above. Therefore examiner reply explained above is also applicable to the rest of these arguments.

Appellant final argument is regarding the dependent claims, that are depending on to the respective independent claims.

**Appellant argued that** since the independent claims are allowable therefore all the claims dependent thereon are also in condition for allowance for the same reasons argued for the independent claim.

**In response to the above argument** by the appellant, **examiner points out** that the respective dependent claims stand or fall with the independent claims.

#### **(11) Related Proceeding(s) Appendix**

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Application/Control Number: 10/084,436

Page 20

Art Unit: 2132

**Samson Lemma**


**S.L.  
12/20/2006**

Conferees:

Kim Vu

KV

Kambiz Zand

  
KAMBIZ ZAND  
PRIMARY EXAMINER